Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer June 2008 | Volume 2, Issue 6

Using Encryption to Protect Data

With major data breaches being reported all too frequently, organizations are now placing increased emphasis on security of personal, private, and sensitive information. One method of increasing security is through data encryption. Encryption is the process of scrambling a message or data so that no one but the sender and the intended recipient can read it. Militaries, businesses, and governments all over the world use it in a variety of ways.

Two general types of encryption are used for cyber security: hardware-based and software-based. Hardware-based encryption is built into a piece of hardware. An example of hardware-based encryption would be the pre-encrypted hard drives that are currently on the market. All data stored on them is automatically encrypted, even the temporary files. A pre-encrypted USB drive is another example of hardware-based encryption. Software-based encryption refers to an encryption program installed on a computer or a server that encrypts either some or all of the data on the system.

With the increasing use of computers in every aspect of our life and the need to protect the information on those computers, the use of encryption has expanded. The following examples illustrate how encryption can be a key component of a defense-in-depth strategy:

- **Laptop protection** – The first use for encryption many people think of is the data on laptop computers. This type of encryption can be done by encrypting specific directories and files or by encrypting the entire hard drive (full disk encryption). Some analysts recommend using both forms of encryption on the same laptop since that is more secure than either method individually. Minimally, file level encryption should be implemented; full disk encryption is a best practice.

- **Wireless networks** – Confidential and valuable data can be intercepted by hackers while being transmitted over wireless networks unless appropriate encryption is employed. Most wireless networks extend far past the walls of the building where they are located. Anyone in the parking lot or on a nearby street may be able to access the wireless network. To prevent unauthorized access, configure wireless networks to employ the appropriate encryption methodology. See the February 2008 Cyber Security Monthly Tips Monthly Newsletter *Securing a Wireless Network* at **www.dir.state.tx.us/security/reading/200802cybersec.htm**.

- **Email and Instant Messaging (IM)** – Email and IM travel through numerous servers and routers before reaching their final destination. They can be intercepted at any stage in this journey and, if they are not encrypted, the data is vulnerable to being accessed. Therefore, do not send confidential or sensitive data via email in clear text or via IM.

- **Backup tapes and media** – Many cases of data breach have resulted from backup tapes and other storage media being lost or stolen. Encrypted these items to prevent unauthorized access.

- **Removable Media** – CDs, DVDs, and USB flash drives are all capable of holding large amounts of data, and these removable devices are being used more frequently. However, be cautious about where these devices are used and of the potential vulnerabilities of using them on an unprotected system. These devices should be encrypted. You can also purchase pre-encrypted USB drives.

- **Smartphones, PDAs, and other similar devices** – These devices can hold a large amount of data. Because of their small size, they can more easily be lost or stolen, putting the data on them at risk. Where practicable, these devices should be encrypted.

A variety of encryption tools are available in the marketplace, some of which are open source. However, please note that any solution you implement should be compliant with accepted industry standards. Given the current technology environment, you should minimally employ a 128-bit Advanced Encryption Standard (AES) solution.

TEXAS COMMON ENCRYPTION WORKING GROUP

DIR has established the Texas Common Encryption Working Group (TCEWG) to address important data protection issues. The TCEWG has a broad representation of state agencies and institutions of higher education to ensure appropriate regulatory and security compliance issues are addressed. The goals of the group are to consolidate feedback on common encryption needs, assess the need for new state encryption policies, and provide recommendations for consideration.

ADDITIONAL RESOURCES

The following sites offer additional guidance regarding encryption:

- Protecting Portable Devices **www.msisac.org/awareness/news/2007-02.cfm**
- Understanding Encryption **http://www.us-cert.gov/cas/tips/ST04-019.html**
- Overview of Encryption: **www.cescomm.co.nz/industry.html**
- Encryption Tutorial: **www.webmonkey.com/programming/php/tutorials/tutorial1.html**

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.

For more information on Internet security, please visit the SecureTexas website – **www.dir.state.tx.us/securetexas**. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by: MS-ISAC www.msisac.org

Powered by: US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM www.us-cert.gov

Distributed by: DIR Secure Texas www.dir.state.tx.us/securetexas

Copyright Carnegie Mellon University | Produced by US-CERT